UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	3:16-CR-35
v.	)	
	)	JUDGES JORDAN/SHIRLEY
THOMAS ALLAN SCARBROUGH,	)	
also known as "Teddybear555,"	)	
	)	
Defendant.	)	

RESPONSE TO DEFENDANT'S OBJECTION TO MAGISTRATE JUDGE'S REPORT AND RECOMMENDATION DENYING MOTION TO SUPPRESS

The United States of America, by and through the United States Attorney, hereby responds to DEFENDANT'S OBJECTION TO MAGISTRATE JUDGE'S REPORT AND RECOMMENTATION DENYING MOTION TO SUPPRESS (Doc. 29) (hereinafter "defendant's Objection") as follows. For the reasons set forth herein and in the United States Response to the defendant's motion to suppress (Doc. 19), incorporated by reference herein, the United States agrees with the Magistrate Judge's conclusion that the evidence seized from the defendant's residence should not be suppressed.

I. INTRODUCTION

The grand jury has charged that defendant Thomas Allen Scarbough distributed and possessed child pornography in October 2015. The evidence leading to the indictment was found on a computer seized from his residence on October 20, 2015, pursuant to a federal search warrant issued in the Eastern District of Tennessee ("the EDTN warrant"). The EDTN warrant was issued based upon probable cause developed through information obtained through a Federal Bureau of Investigation ("FBI") investigation into a child pornography website known as

"Playpen." In association with the investigation of the Playpen website, the FBI had sought and obtained a warrant in the Eastern District of Virginia ("EDVA") permitting it to deploy a "Network Investigative Technique" (the "NIT"). The NIT was employed to cause a computer logging into Playpen to reveal certain identifying information—most importantly, its concealed Internet Protocol ("IP") address. The defendant's computer was one of many computers that connected to the Playpen website and the NIT revealed his IP address to the FBI, leading to the EDTN warrant. Defendant moved to suppress the evidence obtained from his computer on the basis that the NIT Warrant was unauthorized and unconstitutional and that the evidence obtained from his residence was the "fruit of the poisonous tree" in that the EDTN warrant was predicated on the NIT Warrant.

On August 26, 2016, following substantial briefing by both parties and a hearing, the Magistrate Judge concluded in his Report and Recommendation ("R&R") that the Motion to Suppress should be denied. As set out in the parties' briefing and below, several federal courts have already addressed the issues presented in this case:

- whether the NIT Warrant issued in the EDVA was properly authorized under Rule 41 of the Federal Rules of Criminal Procedure;
- whether the NIT Warrant violated the Fourth Amendment to the United States Constitution; and
- if the NIT Warrant was improperly issued, whether suppression should be denied under *Leon* and *Herring* due to the good faith reliance of the law enforcement officers executing the warrant resulting in the seizure of the defendant's computer.

In his R&R, Magistrate Judge Shirley concluded that the Magistrate Judge in the EDVA exceeded her authority in issuing the NIT Warrant under Rule 41 because the NIT Warrant permitted searches to be conducted outside of the EDVA; therefore, because the EDVA Magistrate Judge did not have authority to issue the warrant, Magistrate Judge Shirley concluded that that it violated the Fourth Amendment. R&R at PageID# 378, 380. However, Magistrate Judge Shirley concluded that the evidence should not be suppressed because the agents who executed the EDTN warrant acted in good faith reliance on the EDVA warrant under a *Herring* balancing test. *Id*. at PageID# 389 – 91. Defendant Scarbrough objects to the Magistrate Judge's recommendation that the defendant's Motion to Suppress be denied, disagreeing with Magistrate Judge Shirley's conclusion that the *Herring* balancing test tipped against suppression of the evidence. Doc. 29 at PageID# 409.

II. THE SEARCH WARRANTS LEADING TO THE INDICTMENT

A. The NIT Warrant

The affidavit supporting the NIT Warrant Application (Doc. 19-1) established the need for the NIT to identify Playpen users and set forth ample probable cause to conclude that any users of Playpen knew of its illicit content and intended to access that content. As the affidavit explained, Playpen was a hidden site operating on the Tor network, an anonymous Internet "Dark Web" computer network, and was a website dedicated to the sharing of child pornography. The EDVA magistrate judge reasonably concluded that there was a fair probability that anyone who logged into Playpen did so with knowledge of its content and intent to view that content.

The affiant for the NIT Warrant was a veteran FBI agent with 19 years of federal law enforcement experience and particular training and experience investigating child pornography

and the sexual exploitation of children. NIT Affidavit ¶ 1 (Doc. 19-1, PageID# 128). The NIT Affidavit clearly and comprehensively articulated probable cause to deploy the NIT to obtain IP addresses and other computer-related information that would assist law enforcement in identifying registered Playpen users who were utilizing the Tor's anonymization technology to expose child sexual exploitation on a massive scale.

The NIT Affidavit explained that Playpen was "dedicated to the advertisement and distribution of child pornography," "discussion of … methods and tactics offenders use to abuse children," and "methods and tactics offenders use to avoid law enforcement detection while perpetrating online child exploitation crimes," such as the ones noted in the affidavit. *Id.* at ¶ 10. The affidavit further stated that the "administrators and users of [Playpen] regularly send and receive illegal child pornography via the website." *Id.* The NIT Affidavit also described the massive scale of the site, which appeared to have been operating since August 2014; site statistics indicated that, as of February 3, 2015, it contained 158,094 members, 9,333 message threads, and 95,148 posted messages. *Id*. at ¶ 11.

While the FBI was able to view and document the substantial illicit activity taking place on Playpen, investigators faced a tremendous hurdle in their effort to unmask Playpen users engaging in sexual exploitation of children. Because Playpen was a Tor website, Playpen logs of user activity would contain only the IP address of the last computer through which the communications of Playpen's users were routed (the "exit node") before the communications reached Playpen, which prevented the FBI from identifying the IP address of the Playpen user. IP address logs therefore could not be used to identify and locate Playpen users like the defendant. Accordingly, in order for law enforcement to be able to attain the sort of information

that would identify the users through the ordinary investigative means, the offenders' use of the Tor network necessitated the use of a NIT.

Acting on a tip from a foreign law enforcement agency as well as further FBI investigation, the FBI determined that the computer used to host Playpen was located at a web-hosting facility in North Carolina. FBI agents apprehended the administrator of Playpen in February 2015 and seized the web-hosting facility in North Carolina. Rather than merely shutting the site down, which would have allowed the Playpen users to go unidentified, the FBI interdicted the site and allowed it to continue to operate at a government facility located in the EDVA between February 20, 2015 and March 4, 2015. During that period, the FBI obtained court approval from the United States District Court for the EDVA to monitor site users' communication and deploy the NIT to attempt to identify registered site users who were anonymously engaging in the continuing sexual abuse and exploitation of children, and to locate and rescue children from the imminent harm of ongoing abuse and exploitation. As described in detail in the application for the warrant authorizing its use, the NIT consisted of computer code which, when downloaded along with other content of Playpen by a registered user's computer, was designed to cause the user's computer to transmit a limited set of information – the user's true IP address and other computer-related information – that would assist in identifying the computer used to access Playpen and its user. (*Id.* at ¶¶ 31-37.) The search warrant authorization permitted that minimally invasive technique to be deployed when a registered user logged into Playpen by entering a username and password while the website was being hosted in the EDVA.

B. The Search Warrant for the Defendant's Residence

The NIT revealed the IP address of Playpen user "Teddybear555" and a subpoena was issued to the Internet service provider that operated that IP address. The information obtained from the subpoena revealed that the IP address used by "Teddybear555" was assigned to the defendant's residence. Affidavit of SA Kristina Norris, ¶ 37 (Doc. 14-3 at PageID# 70). Based upon this information, a federal search warrant was obtained for the defendant's residence on October 15, 2015. The affidavit in support of the warrant for the defendant's residence described Playpen in detail and articulated that data obtained from logs on Playpen, court-authorized monitoring by law enforcement, and the court-authorized deployment of the NIT. The information gathered had revealed that Playpen user "Teddybear555" had been logged onto the Playpen website for 20 hours between February 26, 2015, through March 4, 2015. *Id.* at PageID# 68-69, ¶ 30. The affidavit further detailed various posts or discussions which "Teddybear555" had accessed on Playpen during that period. *Id*. at PageID# 69, ¶¶ 31-35.

Law enforcement officers executed the federal search warrant for the defendant's residence on October 20, 2015, and searched the defendant's residence and seized a laptop computer with an internal hard drive. A forensic examination of the hard drive revealed the presence of child pornography, as well as the installation of the Tor software. The defendant was indicted on March 8, 2016.

III. ARGUMENT

A. The NIT Warrant was properly issued by the Magistrate Judge in the EDVA.

For the reasons stated in the Response to the Motion to Suppress, the United States respectfully continues to assert that the NIT Warrant was properly issued by the Magistrate Judge in the EDVA and that this Honorable Court need not resort to a *Leon* good faith analysis to

determine that suppression is unwarranted. *See* Response to Motion to Suppress (Doc. 19) at PageID# 117-21. Several courts have already addressed the suppression of evidence obtained based upon the NIT Warrant. To summarize the decisions to date,[1] four decisions have ruled that the NIT Warrant was properly authorized as a tracking device pursuant to Rule 41(b)(4), and denied motions to suppress. See *United States v. Darby*, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016) (Doc. 21); *United States v. Matish*, No. 4:16-CR-16, 2016 WL 3545776, (E.D. Va. June 23, 2016) (Doc. 25); *United States v. Eure*, No. 2:16-CR-43 (E.D. Va. July 28, 2016) (incorporating *Darby*, authored by same judge) (Exhibit 1); *United States v. Jean*, No. 15-cr-50087 (W.D. Ark. Sept. 13, 2016) (Exhibit 2). In addition to Magistrate Judge Shirley's R&R here, eleven decisions have ruled that, although the NIT Warrant was not properly issued pursuant to Rule 41, suppression is unwarranted. *See United States v. Michaud*, No. 3:14-CR-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016) (Exhibit 3); *United States v. Stamper*, No. 1:15CR109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016) (Exhibit 4); *United States v. Epich,* No.15-CR-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016)(unnecessary to reach the issue of Rule 41 compliance, suppression unwarranted) (Exhibit 5); *United States v. Werdene*, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016) (Exhibit 6); *United States v. Rivera*, No. 2:15-cr-266-CJB-KWR (E.D. La. July 20, 2016) (Exhibit 7); *United States v. Acevedo-Lemus*, No. 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016) (Exhibit 8); *United States v. Adams*, No. 16-cr-011 (M.D. Fla. Aug. 10, 2016) (Exhibit 9); *United States v. Torres*, No. 16-cr-285 (W.D. Tex. Sept. 9, 2016) (Exhibit 10); *United States v. Henderson*, No. 15-cr-565 (N.D. Cal. Sept. 1, 2016) (Exhibit 11); *United States v. Knowles*, No. 15-cr-875

[1] Two of the decisions for the cases cited below have been previously filed with the Court as Supplemental Authorities. The *Matish* decision (Doc. 25) was filed under seal, but is now

(D. S.C. Sept. 14, 2016) (Exhibit 12); *United States v. Ammons*, No. 3:16-cr-00011 (W.D. Ky. Sept. 14, 2016) (Exhibit 13). Three decisions have ruled that the issuing magistrate lacked jurisdiction to issue the NIT Warrant, and that suppression of evidence is required. *See United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016) (Exhibit 14); *United States v. Arterbury*, No. 15-CR-182-JHP (N.D. Okla. May 17, 2016) (Exhibit 15); *United States v. Workman*, No. 15-cr-397 (D. Colo. Sept. 6, 2016) (Exhibit 16).

1. New Decisions Finding NIT Warrant Was Properly Issued

In *United States v. Jean*, No. 15-cr-50087 (W.D. Ark. Sept. 13, 2016), the court denied the defendant's motion to suppress, finding that the NIT comported with Rule 41(b)(4)'s tracking warrant exception. *Id.* at 35. The court determined that the defendant had "electronically travelled" to the EDVA in search of child pornography, where the NIT was deployed. *Id.* The court observed:

> First, the NIT is an "electronic device" within the meaning of 18 U.S.C. § 3117(b), because it is an investigative tool consisting of computer code transmitted electronically over the internet. Second, the purpose of the NIT was to track the movement of "property"—which in this case consisted of intangible "information," something expressly contemplated by the definition in Rule 41(a)(2)(A). The third requirement is that the device be "install[ed]" within the issuing district. As reflected in many of the opinions addressing Judge Buchanan's warrant, the term "install" is problematic, primarily because—in a more traditional scenario—the tracking of tangible property under Rule 41(b)(4) requires the tracking device to be physically attached within the warrant issuing district. But the investigative technique used here was not designed or intended to track a tangible item of physical property. Rather, the NIT was designed to track the flow of intangible property—information—something expressly contemplated by Rule 41(a)(2)(A).

Id. at 33 – 34. The court noted that law enforcement seeks a tracking device because it does not know where the suspect or the evidence of the crime may be located; in such instances,

---

publicly available and a motion to unseal it in this docket is being filed concurrently with this response. The other 16 decisions are attached hereto as Exhibits 1 through 16.

Rule 41(b)(4) authorized the use of electronic tracking devices. *Id.* at 34. The court observed that it would be nonsensical to interpret the Rule to require law enforcement to make application for such a warrant to an unknown magistrate judge in the unknown district. *Id.* at 35. The court concluded that the Rule 41(b)(4) was intended to authorize the very warrant employed by the FBI in EDVA. *Id.*

Here, because of the nature of the anonymization of the Tor, the import of Magistrate Judge Shirley's determination that Rule 41 did not authorize the NIT Warrant is tantamount to determining that technique employed by the FBI to uncover the defendant's IP address could *never* have been authorized by a Rule 41 warrant. As the *Jean* court noted, "such a reading is squarely contradicted by the plain language of Rule 41(a)(2)(A)." *Id.*

The *Jean* court further concluded that, even assuming that the NIT was issued in violation of Rule 41, suppression was not justified. The court noted that the NIT Warrant was constitutionally sufficient because it was supported by probable cause and satisfied the particularity requirement. *Id.* at 37. The Court also observed that an Article III judge could have issued the NIT Warrant. *Id.* at footnote 16 (noting that district judges are not limited by Rule 41(b) and may issue warrants to search property located outside their judicial districts when requirements of the Fourth Amendment are met)(*citing United States v. Fiorito*, 640 F.3d 338, 345 (8th Cir. 2011)). Therefore, the court concluded that the defendant was not prejudiced by the issuance of the NIT Warrant. *Id*. at 37.

Finally, the *Jean* court concluded that the FBI acted in good faith reliance on the NIT Warrant, noting that there was "simply no indication that law enforcement suspected the warrant was lacking in probable cause or sufficient particularity, or that the magistrate judge might lack the jurisdictional authority" to authorize it. *Id.* at 39.

In *United States v. Acevedo-Lemus*, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016), the district judge denied the defendant's motion to suppress a search pursuant to a warrant predicated on the NIT Warrant. The court concluded that the defendant's Fourth Amendment rights were not violated because the defendant had no reasonable expectation of privacy in his IP address. *Id.* at *6. Further, even if the deployment of the NIT was a "search" implicating the defendant's Fourth Amendment rights, the court found that the defendant was not prejudiced by any Rule 41 violation, noting that the FBI could have obtained a NIT Warrant and deployed the NIT in every judicial district in the country. *Id.* Furthermore, the court concluded that, under *Leon*, suppression was not warranted:

> FBI agents were, at every juncture, up front with the magistrate judge about how the NIT worked, what it would seize from "activating computers," and where "activating computers" could be located. (Macfarlane Aff. ¶ 48.) That Rule 41 may not yet be a perfect fit for our technological world does not mean that the FBI agents here acted in bad faith.

Id. at *7.

2. Additional Courts have denied suppression despite finding a Rule 41 violation.

In *United States v. Knowles*, No. 15-cr-875 (D. S.C. Sept. 14, 2016), District Judge Gergel concludes that, although the NIT Warrant exceeded the issuing Magistrate Judge's authority, the evidence should not be suppressed for multiple reasons. Firstly, the court concluded that the warrant was not void *ab initio* because the issuing Magistrate Judge satisfied the constitutional requirements of (1) being neutral and detached and (2) capable of determining whether probable cause existed. *Id*. at 22. Secondly, the court found that the NIT Warrant complied with the Fourth Amendment, in that it was supported by the requirements of probable cause and particularity. *Id.* at 23- 24. The court also found that the FBI acted in good faith reliance on the NIT Warrant based upon the issuing Magistrate Judge's mistaken belief that she

had jurisdiction to issue it. *Id.* at 24. Additionally, the court concluded that the exigent circumstances presented by the fleeting nature of the evidence sought justified the searches conducted outside of the EDVA. *Id.* at 26 – 27. The court observed that the FBI was completely candid with the issuing magistrate, did not deliberately disregard Rule 41, and reasonably relied upon the warrant. *Id.* at 27-28. The court also noted that district judges are not constrained by Rule 41's jurisdictional limitations and, rather, have the authority to issue warrants beyond their districts, as their authority derives from the common law. *Id.* at 33. Thus, the defendant was "in no way prejudiced by a magistrate judge signing the NIT Warrant" instead of a Title III judge and, rather, the defect was "most trivial." *Id.* at 33 - 34. Finally, the court noted that the defendant, because of his use of sophisticated anonymization techniques to hide his location, is estopped from asserting prejudice he caused by purposely hiding his location. *Id.*

In *United States v. Henderson*, No. 15-cr-565 (N.D. Cal. Sept. 1, 2016), the court determined that, although the NIT Warrant technically violated Rule 41, suppression was not warranted because the violation was technical, not constitutional, did not prejudice the defendant, and was executed in good faith. Contrary to the R&R here, the *Henderson* court reasoned that the violation was not of a constitutional nature because the warrant was based upon probable cause and was sufficiently particular. *Id.* at 7. Further, the court in *Henderson* also concluded that the defendant was not prejudiced by the technical violation of Rule 41 because he did not have a reasonable expectation of privacy in his IP address and the FBI could have legally discovered the defendant's IP address without the warrant. *Id.* at 8 – 9. Moreover, like Magistrate Judge Shirley, the *Henderson* court found that the FBI would have reasonably believed that the NIT Warrant complied with Rule 41 and that there was no indication that the

FBI deliberately disregarded Rule 41, which established that the government acted in good faith reliance on it. *Id*. at 9 - 10.

Likewise, in *United States v. Torres*, No. 16-cr-285 (W.D. Tex. Sept. 9, 2016), Senior District Judge David Alan Ezra concluded that the Magistrate Judge in the EDVA did not have the authority under Rule 41 to issue the NIT Warrant, but suppression was unwarranted due to the good faith of the FBI in reasonably relying on the NIT Warrant. *Id.* at 17 – 18. Applying *Herring* analysis, the *Torres* court balanced the costs of suppression versus the benefits and concluded that the benefits of suppression did not outweigh its costs, and declined to suppress the evidence.

> Applying the exclusionary rule here would "exact a substantial social cost for the vindication of Fourth Amendment rights," and could result in the suppression of a significant quantity of evidence currently being used to prosecute individuals who allegedly downloaded child pornography from [Playpen] during a two-week period in 2015.

Id. at 18 (citing *Rakas v. Illinois*, 439 U.S. 128, 137 (1978)).

Also, in *United States v. Ammons,* No. 3:16-cr-00011 (W.D. Ky. Sept. 16, 2016), Senior District Judge Thomas B. Russell, after a thorough analysis of the issue presented here, also found that suppression was inappropriate, despite concluding that the warrant was void *ab initio.* The court concluded that the FBI agents acted in good faith and objectively reasonable on the validity of the NIT Warrant. *Id.* at 19.

Likewise, in *United States v. Adams*, No. 16-cr-11 (M.D. Fla. Aug. 10, 2016), District Judge Paul Byron concluded that, although the EDVA warrant was issued in violation of Rule 41, suppression was not warranted based upon *Leon.* *Id.* at 18.

C. *Leon* good faith exception overrides any technical violation of Rule 41(b).

Suppression is a remedy of last resort. As the majority of courts addressing the NIT Warrant have concluded, even accepting that the NIT Warrant was unauthorized by Rule 41, the evidence should not be excluded. In *Leon*, the Supreme Court held that the exclusionary rule "should be modified so as not to bar the admission of evidence seized in reasonable, good-faith reliance on a search warrant that is subsequently held to be defective." *United States v. Leon*, 468 U.S. 897, 905 (1984). There are, however, four exceptions to the "good faith" rule: (1) if the issuing magistrate was misled by information in the affidavit that the affiant knew or should have known was false; (2) if the issuing magistrate wholly abandoned his judicial role; (3) if the affidavit was so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if the warrant failed to particularize the place to be searched or the things to be seized. *See, e.g., United States v. Van Shutters*, 163 F.3d 331, 338 (6th Cir. 1998). None of the exceptions apply here.

The FBI did not mislead the Magistrate Judge that issued the NIT Warrant; to the contrary, the affiant for the NIT clearly explained the techniques to be employed and the methods by which the FBI expected to obtain the information concerning the IP addresses from the NIT. There was no falsity, deception, omission or other conduct that even *hints* that the FBI misled the issuing Magistrate Judge; rather, if anything, the issuing Magistrate Judge mistakenly (but reasonably) concluded that she had the authority to issue the warrant authorizing the deployment of the NIT. Certainly, the full reach of the NIT was laid out for the issuing Magistrate Judge upon which she granted the application and issued the warrant.

It is only when the deterrent value to law enforcement exceeds the substantial social cost of exclusion of evidence that exclusion of the evidence is warranted. As discussed, the cases

cited by the United States in its response to the defendant's motion to suppress (Doc. 13) and above, a magistrate judge's mistaken belief that she has jurisdiction to issue a warrant, absent any indicia of intentional wrongdoing or reckless conduct by the applicant, does not warrant suppression of evidence. Exclusion of evidence in this case would serve only to punish errors of judges and magistrates without an appreciable effect on law enforcement. *See United States v. Leon*, 468 U.S. at 909, 916. Because the agents acted upon an objectively reasonable good faith belief of the legality of the NIT Warrant, suppression of the evidence in the case of defendant Scarbrough would not logically contribute to deterrence of Fourth Amendment violations occasioned by a magistrate's error of the scope or breadth of her authority to issue the NIT Warrant. *Id*. at 921.

Contrary to the defendant's argument in his Objection that "the FBI at a minimum *should have* and likely did know"[2] that the EDVA magistrate issued the NIT Warrant in violation of the Fourth Amendment and Rule 41, courts around the country have found that the NIT Warrant was authorized by Rule 41 and not issued in violation of the Fourth Amendment, demonstrating that any defect of the NIT Warrant was certainly not clear in October 2015. *Jean* and *Acevedo-Lemus, supra*; *see also, United States v. Darby*, No. 2:16-CR-36, 2016 WL 3189703 (E.D. Va. June 3, 2016); *United States v. Matish*, No. 4:16-CR-16, 2016 WL 3545776 (E.D. Va. June 23, 2016); *United States v. Eure*, No. 2:16-CR-43 (E.D. Va. July 28, 2016) (incorporating *Darby*, authored by same judge). Moreover, the FBI was clearly reasonable in relying upon the information gleaned by the NIT Warrant concerning the defendant's whereabouts when it sought the warrant for his residence in October 2015, prior to any court rulings finding that the NIT Warrant was improperly issued. Defendant's innuendo about the FBI's intentions hardly reach

[2] Defendant's Objection at PageID# 412.

the level of demonstrating intentional wrongdoing or reckless conduct by the agents required for suppression under *Leon.*

On the other hand, the costs of suppression would extract a substantial toll, i.e., allowing society and children to be victimized by viewers and distributors of child pornography, with no identifiable curbing of reasonable police behavior. Therefore, Magistrate Judge Shirley properly concluded that the costs of suppression outweighed the negligible deterrent effect of excluding probative, truthful evidence that was found on the defendant's computer.

IV. CONCLUSION

For the foregoing reasons, the United States respectfully submits that the Court should deny the defendant's Motion to Suppress.

Respectfully submitted this 22nd day of September, 2016.

NANCY STALLARD HARR
UNITED STATES ATTORNEY

By: *s/ Matthew T. Morris*
Matthew T. Morris
Assistant United States Attorney
800 Market Street, Suite 211
Knoxville, Tennessee 37902
(865) 545-4167

CERTIFICATE OF SERVICE

I hereby certify that on September 22, 2016, the foregoing was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. Parties may access this filing through the Court's electronic filing system.

By: *s/ Matthew T. Morris*
Matthew T. Morris
Assistant United States Attorney